

GlobalPlatform: a Secure Dynamic Multi-Application Smart-Card Management

NIST Workshop - July 2003 process of growing evolution.

b. progressive development: evolution.

Marc Kekicheff

GlobalPlatform Technical Director

# GLOBALPLATFORM Process of growing

essive development : evou

rase, expansion

## **Agenda**

Multi Application Smart Cards

**Card Management** 

Interoperability

**Security** 

**Business Models** 

**GlobalPlatform Consortium** 

**Implementations** 

#### GLOBAL PLATFORM TOCKS

## **Case for Multi-Application Cards**

## Today -

Lots of Cards ......



Lots of credit/debit cards ...

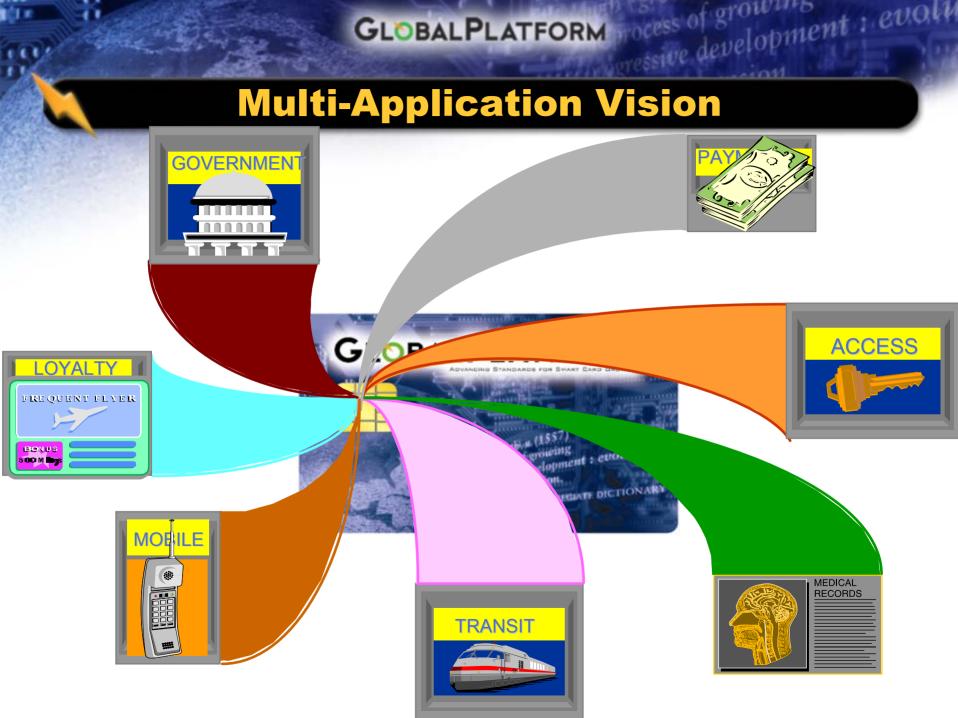
Different pins - different procedures

Different acceptance and capabilities

sive development : evou

Lots of ID cards ....

Different trust and authentication levels Visual evidence of your authorizations, memberships, affiliation



#### GLOBAL PLATFORM TOCCESS

cressive development: evou

## Any Application, Any Time, Any Where

- Multiple Applications on a single card
  - Market Segment of One
- Cross-industry and card schemes interoperability
  - Any type of Application
- Multiple Application Providers on a single card
  - Multiple business partnerships
- Dynamic pre-issuance or post-issuance load / removal of Applications
  - Anytime, Anywhere Access
  - Freedom and choice for cardholders
- Portability of Applications across smart cards
  - → "Write Once, Run Anywhere" TM

#### GLOBAL PLATFORM TOCESS

#### What is an Application?

- Three processors for one Application:
  - Smart card
  - (Card Accepting) Device
  - Host
- Distributed system:
  - Smart card application
  - Device application
  - Host application
- > Relies on an infrastructure

# GLOBALPLATFORM PROCESS OF GROWING

#### **Overall System Components**



Card &

**Application** 

Management

Card



Application specific **Transaction** 



**Systems** 





Device **Application** Management

ressive development : evou

#### GLOBAL PLATFORM TOCKS

## **Managing a Smart-Card System**

- The card is the tip of the iceberg
- The smart card system infrastructure must manage
  - Distributed software among all system components
     Plus
  - Hardware: the smart-card itself
     And
  - Security (distributed over the entire system)
     And
  - Customization (a card is highly personal)
- > A nice IT management challenge...

## GLOBALPLATFORM TOCESS OF BYOLDING

#### **End-To-End Infrastructure**

GlobalPlatform delivers the complete set of smart card specifications for an end to end smart card infrastructure.

Card Specification
Card Compliance Program
Card Security Requirements Spec.



Card Specifications standardize and secure card and application management.

Device API Specification

Device Application Provisioning



Device Specifications enable the acceptance of cards through multiple devices.

Smart Card Management Systems Requirements Profile Specification Scripting Specification



SYSTEMS INFRASTRUCTURE

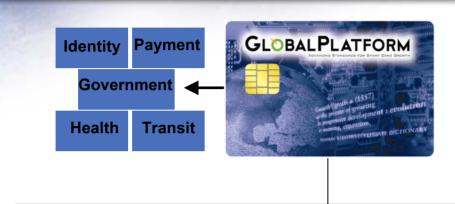
Load & Personalization Spec.

Key Management System Requirements

Systems Specifications standardize back-end systems: personalization, security, key management, application loading.

# GLOBALPLATFORM process of growing evolu-

## Interoperability @ Infrastructure



Compatibility and interoperability among:

**Applications** 

**Cards** 

**Devices** 

**Systems** 













POS

**Mobile Phone** 

**Set Top Box** 

**ATM** 

PC

**PDA** 











Card Management Systems

Application Servers

**Personalization Systems** 

Device Management Systems

Key Management Systems

#### GLOBALPLATFORM TOCESS OF

ressive development : evou

## **Secure Management Framework**

- Secure process:
  - Secure on-card platform
  - Application separation by default
  - Can't load/remove an application without proper authority
  - Authenticity and integrity of application code verified during loading
- Flexible process:
  - Establish clearly roles & responsibilities
  - On-card platform securely manages card and application lifecycle
  - Applications deploy their own security features as need be
- → Wide range of management and relationship models

# GLOBALPLATFORM POCESS OF BROWNE

ressive development : evau

#### **Business Relationship Models**

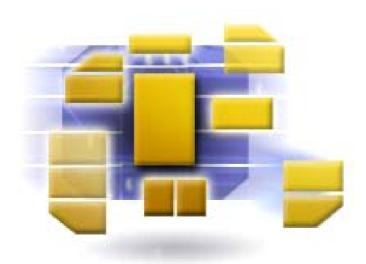
- Allow a multiplicity of trust models:
  - Controlling Authority Model
  - Issuer Centric Model
  - Application Provider Empowered Model
  - Optional on-card "global" Cardholder Verification Method(s)
- Allow a multiplicity of privacy models:
  - Centralized back-office systems (SCMS, transactions, data capture, etc)
  - Distributed back-office systems (SCMS, transactions, data capture, etc)
  - Separation of applications by default (lifecycle, transactions, etc)
  - Limited secured on-card registry
- Open to a multiplicity of business relationships
  - Card Issuer <-> Application Providers
  - Card Issuer / Application Providers <-> Cardholders

# GLOBALPLATFORM Process of growing

ressive development : evou

#### **GlobalPlatform Mission**

Establish an open smart card infrastructure that enables Issuers from many industries to deploy and manage multiple applications through a variety of devices for their customers.



# GLOBALPLATFORM process of growing evolu-

## **Role & Objectives**

Lead the migration from restrictive proprietary environments to an open, interoperable smart card infrastructure

- Meet needs of Issuers from various industries
- Define and promote cross-industry interoperability
- Ensure broad adoption of specifications
- Promote open standards and infrastructure
- Remain relevant by improving technologies



# GLOBALPLATFORM Process of growing

#### Value of GlobalPlatform

#### **Relationship Optimization Tool:**

Delivering the next generation of customer relationship management and customer self-service: leading the move from Customer Management to Customer Empowerment

GlobalPlatform = Interoperability

#### **Customer Empowerment Tool:**

Granting freedom of choice and comparisonthrough a dynamic portfolio of personally relevant, evolving services

essive development : evalu

GlobalPlatform = Scalability



#### **Partnership Tool:**

Allowing the coexistence of multiple applications from multiple business partners through a wide range of relationship models

GlobalPlatform = Security

#### **Cross-Industry Applicability:**

Meeting the diverse needs of Issuers across all sectors-private and public-to deliver customer, constituent and employee based services.

GlobalPlatform = Flexibility

#### **Global Utilization:**

Insuring usage of services and identity, anytime, anywhere through multiple channels and touch points

GlobalPlatform = Portability

#### GLOBALPLATFORM TOCESS OF

essive development : evou

## **Cross-industry Collaboration**

- Close collaboration GlobalPlatform STIP
  - Total convergence
  - Cross-collaboration with FINREAD (eEurope Smart-card Charter)
- Close collaboration GlobalPlatform SCP
  - Around 03.19 and 03.48 GSM & 3G specifications
  - Cross-referencing
- Close collaboration GlobalPlatform NICSS (Japan)
  - MOU
  - Objective: convergence
- Close collaboration GlobalPlatform NIST
  - Dual compliance (e.g. DoD CAC cards)
- Next version of GlobalPlatform Card Spec.
  - Address new SCP technical requests
  - Address new PKI based models (e.g. NICSS)

# GLOBALPLATFORM POCESS OF BROWNE

#### **Implementations**

- GlobalPlatform is used by over 200 million SIMToolKit cards
- Over 20 million GlobalPlatform compliant cards

US Department of Defense



**US Smart Visa** 



**Moscow Social Card** 

ressive development : evou

Taiwan Health Card





and ANZ Bank, Macau SAR, SKT, Sumitomo, Amex Blue, Finland, etc...

Estimation at end of 2003: 40 millions



## THANK YOU

http://www.globalplatform.org

b: progressive development : evolution as the process of growing

e: increase, expansion.

MERRIAM WEBSTER'S COLLEGIATE DICTIONARY